

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA,

v.

BENJAMIN SHACAR,

Defendant.

Criminal Action No. 21-30028-MGM

MEMORANDUM AND ORDER REGARDING  
DEFENDANT'S MOTION TO SUPPRESS  
AND REQUEST FOR A FRANKS HEARING

(Dkt. No. 140)

August 26, 2025

MASTROIANNI, U.S.D.J.

**I. INTRODUCTION**

Benjamin Shacar (“Defendant”) moves to suppress evidence seized by special agents of Homeland Security Investigations (“HSI”) during a March 24, 2021 search of his home in Pittsfield, Massachusetts. As a basis for the requested suppression, Defendant argues the warrant was not supported by probable cause, and therefore the search of his home was unreasonable under the Fourth Amendment to the federal constitution. In an alternative argument, Defendant asserts he is entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) because HSI Special Agent Daniel R. Yon made material misrepresentations and omissions in the affidavit supporting his application for a warrant to search Defendant’s home. The government urges the court to deny both requests, arguing the warrant was plainly supported by probable cause, and that the standard required to obtain a *Franks* hearing has not been met.

For the following reasons, Defendant’s motion to suppress is denied, as is Defendant’s alternative request for a *Franks* hearing.

## II. BACKGROUND<sup>1</sup>

In August of 2019, a foreign law enforcement agency (“FLA”) notified the Federal Bureau of Investigation that it had identified an IP address in the United States that was “used to access online child sexual abuse and exploitation material.” (Dkt. No. 147-3 at 3.)<sup>2</sup> This tip further indicated the website accessed by the IP address (the “targeted site”) was a chat site, known to facilitate the sharing of child sexual abuse and exploitation material depicting victims between the age of 5 and 13 years old. *Id.* Access to the website required creation of a username and password. *Id.* The tip did not allege the IP address had created an account to access the website, nor did the tip claim to know if the IP address had proceeded beyond the password protected home page of the website. According to the FLA, this information was gathered pursuant to the agency’s statutory authority under domestic law, following approval from a judicial officer empowered to review requests to conduct electronic surveillance in that country, and at no time were computers or devices in the United States interfered with during the surveillance. (Dkt. No. 147-3 at 4.)

After receiving this tip, HSI issued a subpoena to Charter Communications seeking to unmask the IP address identified by the FLA. Charter identified the IP address as belonging to the Defendant, Benjamin Shacar. Charter’s records associated the IP address with 18 Maple Street in Pittsfield, Massachusetts. A review of public records indicated Defendant listed 18 Maple Street as his home address with the Massachusetts Registry of Motor Vehicles, the United States Postal Service, and the electric company. Finally, physical surveillance confirmed cars jointly registered in Defendant and his

---

<sup>1</sup> Unless otherwise noted, the court derives all background information from the affidavit Special Agent Yon submitted with his warrant application.

<sup>2</sup> The parties and the court are aware of the identity of the FLA. However, all parties have asked that the identity of the FLA remain under seal. The court takes notice that the FLA is based in a democratic nation with a long-standing tradition of adherence to the rule of law, including through oversight by an independent and well-respected judiciary.

wife's names were present at the address.

On March 22, 2021, Special Agent Yon applied for a warrant to search 18 Maple Street, as well as the person of Defendant and his wife. In addition to detailing the FLA's tip and HSI's efforts to confirm Defendant's links to 18 Maple Street, the affidavit in support of the warrant contained detailed information regarding the process for accessing the targeted site. The site was not freely discoverable via a conventional search engine—like Google—but rather was only available through the Tor network. The Tor network is computer network specifically designed to facilitate anonymous internet usage. A user must download the Tor software; this software enables access to both classic websites and so-called “hidden services” websites. Hidden services websites, commonly called “onion sites,” are only accessible to individuals using Tor. Unlike a traditional website, a Tor-based website is denoted by a 16 or 56 character tagline, followed by the suffix “.onion.” These sites are difficult for law enforcement to trace using traditional tools, as their IP addresses are not searchable in a Domain Name System listing and their servers route all communications through multiple intermediaries to mask location data.

In this specific case, the target website was a Tor hidden services website. Once users obtained the site's Tor specific web address, they would be brought to a home page containing a log in screen. (Dkt. No. 147-3 at 7; Dkt. No. 147-1 ¶¶ 17-18.) The log in screen also contains a text box with a description written in both Cyrillic script and English. In English, the text reads as follows:

Behave and be respectful. Don't demand, don't spam. Follow the requests of the Members. Post links with good photos and videos (preview is required!) No hurtcore, No gore, No zoo, No death, No toddlers. Only GIRLS 4 to 14 years. Any language allowed.

Federal agents subsequently confirmed that, if one registered and made an account, clicking past the log in screen would allow for the viewing of child sexual abuse and exploitation materials.

Based on this affidavit, United States Magistrate Judge Katherine A. Robertson authorized a search warrant for 18 Maple Street, the Defendant's person, and the person of his wife. This warrant

was executed on March 24, 2021. During execution of the warrant, Defendant was read his *Miranda* rights and interviewed by law enforcement. (Dkt. No. 2-1 at 27.) Defendant identified his personal laptop to federal agents, and the Tor browser was subsequently found downloaded on his device. Defendant also admitted downloading child exploitation materials from the internet, and confirmed he saved certain materials to a thumb drive. Defendant told the agents where to find the thumb drive and, after a brief review, HSI identified approximately 80 videos containing child exploitation material. Following this search, Defendant was arrested and subsequently indicted on ten counts of receiving child pornography in violation of 18 U.S.C. § 2252A(a)(2)(A) and one count of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B).

### III. DISCUSSION

#### A. Probable Cause

The Fourth Amendment generally forbids the issuance of any warrant without a showing of probable cause. U.S. Const. amend. IV. In this case, Defendant challenges the probable cause supporting the March 24, 2021 search on two grounds. He first contends the FLA's tip to U.S. law enforcement was insufficient to establish probable cause. Defendant next argues HSI's decision to wait twenty-two months after receiving the FLA tip before searching 18 Maple Street rendered the warrant stale. While the court ultimately finds neither argument persuasive, it will address each in turn.

“Probable cause exists when the facts and circumstances as to which police have reasonably trustworthy information are sufficient to warrant a person of reasonable caution in the belief that evidence of a crime will be found.” *United States v. Dion*, 859 F.3d 114, 131-32 (1st Cir. 2017) (internal quotation marks omitted); *see also United States v. Rondeau*, 626 F. Supp. 3d 403, 415 (D. Mass. 2022) (citing *United States v. Aguirre*, 839 F.2d 854, 857-858 (1st Cir. 1988)). In the context of a search warrant, “[t]he probable cause inquiry is two-fold: ‘[a]n application for a warrant must demonstrate

probable cause to believe that (1) a crime has been committed -- the commission element, and (2) enumerated evidence of the offense will be found at the place searched -- the so-called nexus element.” *United States v. Pyrtle*, 770 F. Supp. 3d 330, 341 (D. Mass. 2025) (quoting *United States v. Gonzalez*, 113 F.4th 140, 148 (1st Cir. 2024)) (internal quotation marks omitted). The nexus requirement “can be inferred from the type of crime, the nature of the items sought, . . . and normal inferences as to where a criminal would hide [evidence of a crime].” *United States v. Corleto*, 56 F.4th 169, 175 (1st Cir. 2022) (internal quotation marks omitted and alterations in original).

When reviewing the sufficiency of an affidavit relied upon by a magistrate judge, this court exercises “an ample amount of deference to the issuing magistrate’s finding of probable cause.” *United States v. Dixon*, 787 F.3d 55, 58 (1st Cir. 2015). Therefore, reversing the magistrate judge’s initial determination is only appropriate if there is “no substantial basis for concluding that probable cause existed.” *Id.* at 58-59.

#### 1. *The FLA’s Tip*

Defendant argues “[t]here is no claim that Shacar spent more than a second on the site, that he registered as a user, that he gained access to any files on the site, that he purchased anything on the site, that he downloaded anything from the site, that he followed a link on the site, or that he ever returned to the site,” but this position blurs the distinction between the probable cause required to arrest (not at issue here) and the probable cause required to search for contraband. In the context of a search warrant, the appropriate inquiry asks whether “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238 (1983). And here, Congress made the well-reasoned decision to completely prohibit access to, or the viewing of, child pornography. By doing so, such material necessarily becomes *per se* contraband and evidence of a crime. Accordingly, the tip provided by the FLA was more than sufficient to satisfy the probable

cause requirement applicable to a search warrant, as it was self-evident just from the log in screen of the targeted website that any internet device used to access the site was reasonably likely to contain (or have viewed) child pornography. *See United States v. Anzalone*, 923 F.3d 1, 5 (1st Cir. 2019) (“[T]he totality of the information asserted in the warrant affidavit – Playpen’s hidden nature on the Tor Network, its registration requirement, its focus on anonymity, and the image depicted on its homepage -- established the fair probability that users went into Playpen to access child pornography.”). The steps required to access the site are, moreover, such that no ordinary individual would stumble upon the website accidentally, meaning the mere fact that Defendant’s IP address visited the home page is further indicia his computer contained contraband. Based on the totality of the circumstances, Judge Robertson had a “substantial basis” to believe any device associated with the IP address in question likely contained evidence of a crime. *United States v. Dixon*, 787 F.3d 55, 58-59 (1st Cir. 2015).

Relying on case law discussing the veracity of tips from informants, Defendant also urges the court to find the affidavit in support of the warrant failed to establish the reliability of the FLA’s tip. To determine an informant’s credibility, the court considers the following non-exhaustive factors:

(1) whether the affidavit establishes the probable veracity and basis of knowledge of persons supplying hearsay information; (2) whether an informant’s statements reflect first-hand knowledge; (3) whether some or all of the informant’s factual statements were corroborated wherever reasonable or practicable (e.g., through police surveillance); and (4) whether a law enforcement affiant assessed, from his professional standpoint, experience, and expertise, the probable significance of the informant’s provided information.

*United States v. Tiem Trinh*, 665 F.3d 1, 10 (1st Cir. 2011) (citations omitted).

Assuming without deciding that the traditional framework for analyzing an informant’s tip is appropriate when analyzing a tip from an FLA,<sup>3</sup> the court concludes the lengthy history of close

---

<sup>3</sup> The First Circuit has not addressed the appropriate framework for analyzing a tip from an FLA. *Cf. United States v. O’Connell*, No. 2:19-CR-00017-GZS, 2019 WL 2396560, at \*5 n. 7 (D. Me. June 6, 2019) (“Although the First Circuit does not appear to have used the traditional tip framework to

cooperation between this specific FLA and the United States Government supports Judge Robertson’s decision to credit the reliability of the tip. *See United States v. Kiejzo*, No. CR 4:20-40036-TSH, 2023 WL 2601577, at \*3 (D. Mass. Mar. 21, 2023) (rejecting a nearly identical argument); *see also United States v. Bateman*, No. 1:20-CR-10012-IT, 2022 WL 980075, at \*3 (D. Mass. Mar. 31, 2022) (same). Specifically, a tip from one well-established law enforcement agency to another “implies a degree of expertise and a shared purpose in stopping illegal activity,” *Bateman*, 2022 WL 980075, at \*3 (quoting *United States v. Benoit*, 730 F.3d 280, 285 (3d Cir. 2013)); the “working relationship’ between the United States and the FLA ‘bolsters the credibility of the information’ since the FLA’s ‘reputation can be assessed,’ and it ‘can be held responsible if its allegations turn out to be fabricated,’” *id.* (quoting *Benoit*, 730 F.3d at 285); and this FLA was not only well known to HSI, but it was also “a repeat-player in the United States’ efforts at combatting child exploitation,” *id.* (internal quotation marks omitted). Based on the totality of the circumstances surrounding the tip, there was a substantial basis for Judge Robertson to conclude the FLA’s information reliably supported probable cause.

## 2. *Staleness*

The court is also not persuaded by Defendant’s alternative argument that the twenty-two-month delay between the alleged access and the search rendered probable cause lacking. The First Circuit “has repeatedly refused to assess an affidavit’s staleness by counting the number of days between the events described in the affidavit and a warrant’s issuance, as a merchant would beads on an abacus.” *United States v. Tiem Trinh*, 665 F.3d 1,13 (1st Cir. 2011). Rather, the staleness inquiry turns on “the nature of the information, the nature and characteristics of the suspected criminal activity,

---

analyze the reliability of information passed between law enforcement officers, the Court discerns no precedent indicating that courts cannot do so.”). Other courts addressing the question have also generally bypassed the question and proceeded to decide the issue under the classic framework. *See, e.g., United States v. Benoit*, 730 F.3d 280, 285-86 (3d Cir. 2013); *United States v. Kiejzo*, No. CR 4:20-40036-TSH, 2023 WL 2601577, at \*2-3 (D. Mass. Mar. 21, 2023).

and the likely endurance of the information.” *Id.* at 14 (internal quotation marks omitted).

Applying these factors, the twenty-two-month delay did not render it less likely that officers would find evidence of the offense, meaning the delay did not impact probable cause. It is well-established in federal law “that customers of child pornography sites do not quickly dispose of their cache.” *United States v. Morales-Aldabondo*, 524 F.3d 115, 119 (1st Cir. 2008); *see also United States v. McLellan*, 792 F.3d 200, 209 n. 5 (1st Cir. 2015) (“[C]ourts have held time and time again that child pornography traders and collectors maintain their collections for long periods of time, and often store it in safe, close, and easily accessible locations”). In accordance with this rule, courts have refused to find staleness when assessing delays of a similar (or longer) lengths of time. *United States v. Morales-Aldabondo*, 524 F.3d 115, 119 (1st Cir. 2008) (more than three-year delay); *United States v. Kiejzo*, No. CR 4:20-40036-TSH, 2023 WL 2601577, at \*3 (D. Mass. Mar. 21, 2023)(sixteen month delay acceptable); *United States v. Rondeau*, 626 F. Supp. 3d 403, 417 (D. Mass. 2022) (collecting cases finding lack of staleness after two- and five-year delay); *United States v. Irons*, 594 F. Supp. 3d 171, 179 (D. Mass. 2022) (one-year delay acceptable). Special Agent Yon’s affidavit clearly informed Judge Robertson of the characteristics unique to individuals possessing child pornography, including their proclivity to maintain the images for many years, Judge Robertson then appropriately weighed these characteristics in finding probable cause. (Dkt. No. 147-1 ¶ 54.) The court agrees that, in the circumstances of this case, the twenty-two-month delay did not render the information stale.

Accordingly, Defendant’s motion to suppress is denied in its entirety.

## **B. Franks Hearing**

In a final argument, Defendant contends he is entitled to a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). Under *Franks*, “a defendant may request an evidentiary hearing to challenge the truthfulness of statements made by law enforcement agents in a search warrant



affidavit.” *United States v. Hicks*, 575 F.3d 130, 138 (1st Cir. 2009). To obtain an evidentiary hearing, Defendant must make a “substantial preliminary showing” that (1) the affidavit accompanying the warrant contains false statements or omissions made “knowingly and intentionally, or with reckless disregard for the truth,” and (2) these false statements or omissions were necessary to the finding of probable cause. *Id.* (quoting *Franks*, 438 U.S. at 155-56).

Defendant’s motion raises two issues potentially justifying a *Franks* hearing: (1) an alleged misrepresentation by Agent Yon as to the nature, origin, and reliability of the FLA’s tip; and (2) Agent Yon allegedly made material omissions regarding the method used by the FLA to identify Defendant’s IP address. After careful consideration, the court is persuaded neither of these asserted misrepresentations or omissions satisfies Defendant’s burden to obtain a *Franks* hearing.

As to the first grounds, the court finds Special Agent Yon’s rephrasing of the tip was minor and did not constitute a misrepresentation in the affidavit. (*Compare* Dkt. No. 147-1 ¶¶ 32-33, *with* Dkt. No. 147-3 at 3.) If anything, Yon’s paraphrasing more clearly conveyed the tip’s meaning than the language of the FLA’s letter itself. Similarly, Yon did not misrepresent the contents of the target website’s home page, as Paragraphs 8-23 extensively detailed the steps an individual would need to take to access the website and provided an extensive (and accurate) depiction of the contents of the home page. This description was, as the court previously found, more than sufficient for a neutral magistrate to conclude probable cause existed to search Defendant’s electronic devices. *See, e.g., United States v. Kiejzo*, No. CR 4:20-40036-TSH, 2023 WL 2601577, at \*4-5 (D. Mass. Mar. 21, 2023) (rejecting substantially the same argument); *United States v. Bateman*, No. 1:20-CR-10012-IT, 2022 WL 980075, at \*4 (D. Mass. Mar. 31, 2022) (same).

Turning to the alleged omission, Defendant relies on an expert affidavit submitted in an unrelated case in the Eastern District of Virginia. According to this affidavit, there are only two possible methods for identifying IP addresses using the Tor browser—traffic analysis or network

investigative technique. The affidavit further indicates the first approach is prone to errors, while the second technique interferes with the user's computer. Thus, Defendant posits Yon's failure to identify the technique used misled Judge Robertson by either (i) using a faulty, error prone method, or (ii) by falsely stating the FLA never interfered with a computer in the United States. This same argument, relying on the same Eastern District of Virginia affidavit, has been considered and rejected by multiple courts in this district as pure speculation. *See United States v. Kiejzo*, No. CR 4:20-40036-TSH, 2023 WL 2601577, at \*6-7 (D. Mass. Mar. 21, 2023); *United States v. Bateman*, No. 1:20-CR-10012-IT, 2022 WL 980075, at \*5 (D. Mass. Mar. 31, 2022) (same). It was also rejected by the Fourth Circuit and the Eastern District of Virginia in the case in which the affidavit was filed. *See United States v. Sanders*, 107 F.4th 234, 254 (4th Cir. 2024), *cert. denied*, 145 S. Ct. 1434, 221 L. Ed. 2d 557 (2025). The court agrees with these well-reasoned decisions, as it is pure speculation that the FLA interfered with a computer in the United States.<sup>4</sup>

Accordingly, Defendant's motion for a *Franks* hearing is denied.

#### IV. CONCLUSION

For the foregoing reasons, Defendant's motion to suppress and motion for a *Franks* hearing are DENIED. (Dkt. No. 140.)

It is So Ordered.

/s/ Mark G. Mastroianni  
MARK G. MASTROIANNI  
United States District Judge

---

<sup>4</sup> The court also agrees with the *Kiejzo* Court, even if there was a misrepresentation, it was not material because "searches conducted by FLAs are not subject to the exclusionary rule, even when they are conducted on American soil." *Id.* at \*7-9.